CLAIMS

I Claim:

1. A system for detecting and restricting denial of service attacks, comprising:

a transmit algorithm to receive packets from a software application and discard packets that are determined to be from a zombie application;

a receive algorithm to receive packets from a network interface and discard packets that are determined to be from a zombie application; and

a monitor code in communications with the transmit algorithm and the receive algorithm to track the pattern of packet transmission and reception to and from the software application and determine that the software application is a zombie application based upon the pattern of packet transmission and reception.

2. The system recited in claim 1, wherein said monitor code determines that the software application is the zombie application by identifying that the software application is transmitting a large number of packets without receiving any packets and placing the software application on a zombie list or a watch list.

3. The system recited in claim 2, wherein said monitor code alerts the user and the transmit algorithm and receive algorithm that a software application is a zombie application when the software application has previously been placed on the zombie list or the watch list and the software application is still transmitting a large

number of packets without receiving any packets.

4. The system recited in claim 1, wherein said monitor code determines that the software application is the zombie application by identifying that the software application is not receiving any packets and placing the software application on a watch list.

5. The system recited in claim 4, wherein said monitor code alerts the user and the transmit algorithm and receive algorithm that a software application is a zombie application when the software application has previously been placed on the watch list and the software application is now transmitting a large number of packets.

6. The system recited in claim 1, wherein said monitor code determines that the software application is a possible zombie application by identifying that the software application is rarely receiving any packets and placing the software application on a watch list.

7. The system recited in claim 6, wherein said monitor code alerts the user and the transmit algorithm and receive algorithm that a software application is a zombie application when the software application has previously been placed on the watch list and the software application is now transmitting a large number of packets.

8. The system recited in claim 1, wherein said monitor code determines

that the software application is a possible zombie application by identifying that the software application has stopped receiving any packets or receiving packets and placing the software application on a watch list.

9. The system recited in claim 8, wherein said monitor code alerts the user and the transmit algorithm and receive algorithm that a software application is a zombie application when the software application has previously been placed on the watch list and the software application is now transmitting a large number of packets.

10. The system recited in claim 3, wherein said monitor code will retain an application on the watch list when a zombie rating exceeds a predetermined value, said zombie rating is based on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.

11. The system recited in claim 5, wherein said monitor code will retain an application on the watch list when a zombie rating exceeds a predetermined value, said zombie rating is base on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup..

12. The system recited in claim 7, wherein said monitor code will retain an application on the watch list when a zombie rating exceeds a predetermined value,

said zombie rating is base on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.

13. The system recited in claim 9, wherein said monitor code will retain an application on the watch list when a zombie rating exceeds a predetermined value, said zombie rating is base on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.

14. A method of detecting and restricting denial of service attacks, comprising:

monitoring incoming and outgoing packets to and from a software application;

placing said software application on a zombie list or a watch list when a pattern of the incoming or outgoing packets from the software applications matches that of the characteristics of a zombie application; and

blocking reception and transmission of packets to the software application when the software application has been placed on the watch list or the zombie list in a previous cycle and the software application further exhibits the characteristics of a zombie application.

15. The method recited in claim 14, wherein the characteristics of a zombie application are transmitting a large number of packets while receiving no incoming packets.

16. The method recited in claim 14, wherein the characteristics of a zombie application are receiving no incoming packets and having a zombie rating exceeding a predetermined value.

17. The method recited in claim 16, wherein said zombie rating is based on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.

18. The method recited in claim 14, wherein the characteristics of a zombie application are rarely receiving incoming packets and having a zombie rating exceeding a predetermined value.

19. The method recited in claim 18, wherein said zombie rating is based on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.

20. The method recited in claim 14, wherein the characteristics of a zombie application are receiving incoming packets at first and then not receiving or sending any packets and having a zombie rating exceeding a predetermined value.

21. The method recited in claim 20, wherein said zombie rating is based on the factors of whether the software application is an application or a process and

whether the application is user initiated or initiated at system startup.

22. A computer program, comprising:

monitoring incoming and outgoing packets to and from a software application;

placing said software application on a zombie list or a watch list when a pattern of the incoming or outgoing packets from the software applications matches that of the characteristics of a zombie application; and

blocking reception and transmission of packets to the software application when the software application has been placed on the watch list or the zombie list in a previous cycle and the software application further exhibits the characteristics of a zombie application.

23. The computer program recited in claim 22, wherein the characteristics of a zombie application are transmitting a large number of packets while receiving no incoming packets.

24. The computer program recited in claim 23, wherein the characteristics of a zombie application are receiving no incoming packets and having a zombie rating exceeding a predetermined value.

25. The computer program recited in claim 22, wherein said zombie rating is based on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.

26. The computer program recited in claim 25, wherein the characteristics of a zombie application are rarely receiving incoming packets and having a zombie rating exceeding a predetermined value.

27. The computer program recited in claim 26, wherein said zombie rating is based on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.

28. The computer program recited in claim 22, wherein the characteristics of a zombie application are receiving incoming packets at first and then not receiving or sending any packets and having a zombie rating exceeding a predetermined value.

29. The computer program recited in claim 28, wherein said zombie rating is based on the factors of whether the software application is an application or a process and whether the application is user initiated or initiated at system startup.